EPSTEIN BECKER GREEN

Employment, Labor & Workforce Management

ACT NOW ADVISORY

Unemployment Insurance Fraud: What to Do When It Strikes Your Business and Workers

March 2, 2021

By Steven M. Swirsky, Tzvia Feiertag, Jillian de Chavez-Lau, and Brian G. Cesaratto

---

As the COVID-19 pandemic wears on, and as states race to keep up with unprecedented volumes of claims for unemployment insurance ("UI") benefits and relax certain requirements, like waiting periods, scam artists and criminals are filing billions of dollars' worth of fraudulent claims to steal funds intended to aid workers who have lost their jobs in this difficult environment. In New York alone, officials have identified more than 500,000 fraudulent unemployment insurance claims, totaling $5.5 billion in claims. And in California, officials have identified at least $11.4 billion in fraudulent claims, and suspect an additional $20 billion may be fraudulent. Other states, including Ohio, Colorado, and Maryland, have also flagged millions of dollars more in improper claims.

UI fraud occurs when imposters using other people's names and personal information (typically gained through improper means, such as data breaches or social engineering attacks) attempt to claim unemployment benefits they are not entitled to. In many cases, people discover that they've been targeted for UI fraud only after the fact, when (i) they apply for unemployment benefits and learn that a claim has already been opened in their name; (ii) they receive a notice from their state's unemployment agency that a claim has been opened in their name; (iii) their employer informs them that someone has filed for unemployment benefits in their name; (iv) after their unemployment benefits account has been funded, fraudsters call, text, or email them to try to divert the money to them, or they impersonate agents from the state UI agency saying that the money was sent by mistake and should be repaid; or (v) they receive a Form 1099-G reporting unemployment income that is subject to federal income tax. Similarly, an employer may learn that it has been affected by UI fraud when its employees alert it to suspicious UI claims; the employer receives notices from the state unemployment agency to that effect; when the employer receives notices that claims have been filed by or on behalf of persons who remain actively employed; or when the employer notices unusually large amounts being charged against its UI accounts and quarterly statements seeking payment of the employer share.

If a business learns of or suspects UI fraud, it should move quickly to gather all relevant information to investigate the fraud, notify the appropriate authorities, and formulate a plan to address the fraud's financial impact on the business and employees' identity theft concerns:

1. *Gather information to determine the details and scope of the UI fraud*. If an employee tells their employer that they may or have been targeted by UI fraud, the employer should promptly investigate the matter. In addition to gathering the facts from the employee, employers should check to see if they have received notices of claims for benefits that appear suspicious once compared against employee records (e.g., claims made in the names of active employees, or claims filed in the names of former employees who are known to be currently working for another employer or elsewhere).

More generally, and regardless of whether employees have reported actual or suspected UI fraud, employers should pay close attention to unemployment charge benefits statements they receive from the state. In New York, for example, employers receive quarterly unemployment insurance statements from the Department of Labor. Amounts charged to the employer in one quarter that are significantly higher than previous comparable pre-pandemic quarters may be an indication of UI fraud.

If charges appear on an employer's UI account, but the employer can present other indicia of suspected UI fraud, depending on the state, it may be possible to negotiate with the state for a lower, good-faith payment based upon the employer's payment history for previous comparable quarters, and an agreement that neither interest nor penalties will accrue while potential UI fraud is being investigated. (Before making any payment, employers should evaluate whether there is any portion of UI charges that they are not liable for based on federal or state law. For example, reimbursable employers—such as not-for-profits and government entities—should keep in mind that under the Coronavirus Aid, Relief, and Economic Security ("CARES") Act and the Continued Assistance Act, the federal government covers 50 percent of the costs of reimbursable employer charges. And for these types of employers based in New York, on January 14, 2021, Roberta Reardon, Commissioner of the New York State Department of Labor signed an order ("Order") providing that the state will reimburse the employer for the remaining 50 percent of charges. Furthermore, the January 14 Order provides that, for all employers—regardless of whether the employer pays UI taxes based on experience ratings or directly reimburses the state of UI benefits paid to claimants—*all* UI benefits paid to claimants beginning on March 9, 2020, will be charged to the state's general UI account, and not attributable to employers. At the moment, this appears to cover amounts owing to UI fraud as well.)

2. *Promptly report suspected UI fraud*. The employer and affected employee should immediately report suspected UI fraud to the Federal Trade Commission ("FTC"), the state unemployment benefits agency, and local law enforcement. The U.S. Department of Labor provides guidance on how to report unemployment fraud in each state, and some states (like New York) have dedicated websites to report UI fraud. In addition, many local district attorney's offices (like Nassau County, New York) have set up websites for the reporting of such fraud.

3. *Support affected employees' efforts to report UI fraud, and address identity theft concerns.* Employers should have a plan to communicate steps employees can take to respond to UI fraud, and to ensure them that the business takes claims of UI fraud very seriously. Employers should consider including in their plan:

- **General information about the prevalence of UI fraud and who to contact at work if employees believe or find out they've been victims of these scams.**

- **Steps that employees can take to protect their finances and credit (see the FTC's recommendations here).** These steps should include (i) reporting identity theft to the FTC, credit bureaus, state agencies, local law enforcement, and the employees' banks, and (ii) protecting against future fraudulent use of the employees' personal information, such as regularly reviewing their credit reports, placing fraud alerts on their credit, or freezing their credit. Employers should suggest that employees visit the FTC's IdentityTheft.gov website, which guides individuals through these steps.

  Employers should also check for new initiatives by state authorities to help employees. In New York, for example, on February 25, 2021, Governor Andrew Cuomo announced the launch of the Department of Labor's new webpage, which, in addition to providing online forms to report UI fraud and identity theft to the state and to the FTC, outlines ways individuals can combat identity theft.

- **Resources for situations where an employee has received a Form 1099-G in connection with a fraudulent UI clam.** The Internal Revenue Service ("IRS") currently advises affected individuals to request a revised Form 1099-G from the issuing state agency showing that they did not receive employment benefits. However, questions remain with respect to the IRS's plan for addressing this issue, such as how the IRS plans to review 2020 income tax returns affected by UI fraud (or identify theft in general), or whether refunds might be delayed if a return is flagged for Form 1099-G unemployment compensation. Recently, members of Congress have asked the IRS to release additional guidance on these and other issues related to unemployment fraud.

4. *Perform a cybersecurity assessment*. When faced with possible UI fraud, employers should immediately consult with their IT and/or cybersecurity teams to determine whether their systems may have been breached, resulting in unlawful access to employees' personal identifying information. Cybercriminals are always looking for ways to monetize identity theft, and unemployment insurance fraud scams are one widespread means of doing so. A series of fraudulent unemployment claims may be a leading indicator of a data breach compromising employee personal information, particularly when there is a series of claims in close proximity. Indeed, the FBI has seen a spike in unemployment insurance fraud during the COVID-19 pandemic due to computer intrusions and data breaches. In general, employers should evaluate their cybersecurity safeguards on an ongoing basis. Employers should also be especially vigilant in securing remote access as a result of the increased numbers of employees working remotely during the pandemic and follow cybersecurity best practices.

****

For more information about this Advisory, please contact:

Steven M. Swirsky
New York
212-351-4640
sswirsky@ebglaw.com

Tzvia Feiertag
Newark
973-639-8270
tfeiertag@ebglaw.com

Jillian de Chavez-Lau
New York
212-351-4735
jdechavezlau@ebglaw.com

Brian G. Cesaratto
New York
212-351-4921
bcesaratto@ebglaw.com

About Epstein Becker Green
Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in locations throughout the United States and supporting domestic and multinational clients, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.